AMENDMENT TO THE CLAIMS

1–20. (Cancelled)

21. (Previously presented) An encryption/decryption device comprising:

a data structure analysis block for receiving encrypted data or data to be encrypted, analyzing the structure of the data and outputting information related to encryption as control data, the data structure analysis block also outputting the encrypted data or the data to be encrypted as processing block input data;

a data control block for outputting an encryption/decryption switch signal indicating which one of encryption and decryption should be performed, and a mode selection signal indicating in which mode the processing block input data should be processed, according to the control data; and

a shared processing block configured to have the ability to perform encryption and decryption in either of the Cipher Block Chaining (CBC) mode and the Cipher Feedback (CFB) mode by performing Electronic Code Book (ECB) processing using input key data, the shared processing block performing encryption or decryption according to the encryption/decryption switch signal for the processing block input data in the mode indicated by the mode selection signal, and outputting encrypted result or decrypted result,

wherein the shared processing block comprises:

an ECB processor for performing the ECB processing and outputting the result as cipher-processed data;

a first selector for selecting one of the processing block input data and the cipher-processed data according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data;

a delay device for delaying the processing block input data and the cipher-processed data received as inputs and outputting the delayed data;

a second selector for selecting one of the processing block input data, initial vector data, and the delayed processing block input data and the delayed cipher-processed data output from the delay device according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data;

an XOR operator for computing XOR of the output of the first selector and the output of the second selector and outputting the computed result;

a third selector for selecting one of the processing block input data, the output of the XOR operator, the delayed processing block input data and the delayed cipher-processed data according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data;

a bit mask device for masking part of the key data as required according to the mode selection signal and outputting the result as mode-adaptive key data; and

a fourth selector for selecting one of the cipher-processed data and the output of the XOR operator according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data as the encrypted result or the decrypted result, and

the ECB processor performs either encryption or decryption as the ECB processing for the output of the third selector using the mode-adaptive key data according to the encryption/decryption switch signal and the mode selection signal, and outputs the result as the cipher-processed data.

22. (Previously presented) The encryption/decryption device of Claim 21, wherein the data structure analysis block analyzes a header of the encrypted data to draw out a Media Access Control (MAC) structure from the encrypted data based on information in the header, and if an extension header exists in the MAC structure and the extension header indicates that the encrypted data has been encrypted, the data structure analysis block outputs information related to encryption included in the extension header as the control data, and also removes the extension header from the MAC structure data and outputs the result as the processing block input data.

23. (Previously presented) The encryption/decryption device of Claim 21, wherein the data control block outputs a signal indicating in which mode, the CBC mode or the CFB mode, the processing block input data should be processed and in which key data length mode the data should be processed, as the mode selection signal, according to the control data.

24. (Previously presented) The encryption/decryption device of Claim 21, wherein the bit mask device outputs the key data as it is if the mode selection signal indicates a 56-bit key mode, or otherwise masks unnecessary bits and outputs the resultant data, as the mode-adaptive key data.

25. (Previously presented) The encryption/decryption device of Claim 21, wherein the first selector selects the processing block input data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, or otherwise selects the cipher-processed data, and outputs the selected data.

26. (Previously presented) The encryption/decryption device of Claim 21, wherein the second selector selects the initial vector data at start of processing and thereafter selects the delayed cipher-processed data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, and outputs the selected data,

selects the initial vector data at start of processing and thereafter selects the processing block input data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CFB mode, and outputs the selected data,

selects the initial vector data at start of processing and thereafter selects the delayed processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CBC mode, and outputs the selected data, or

selects the initial vector data at start of processing and thereafter selects the processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CFB mode, and outputs the selected data.

27. (Previously presented) The encryption/decryption device of Claim 21, wherein the third selector selects the output of the XOR operator if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, and outputs the selected data,

selects the processing block input data at start of processing and thereafter selects the delayed cipher-processed data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CFB mode, and outputs the selected data,

selects the processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CBC mode, and outputs the selected data, or

selects the processing block input data at start of processing and thereafter selects the delayed processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CFB mode, and outputs the selected data.

28. (Previously presented) The encryption/decryption device of Claim 21, wherein the fourth selector selects the cipher-processed data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, and outputs the selected data,

selects the output of the XOR operator if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CFB mode, and outputs the selected data, or

selects the output of the XOR operator if the encryption/decryption switch signal indicates decryption, and outputs the selected data.

29. (Previously presented) The encryption/decryption device of Claim 21, wherein the ECB processor performs encryption if the encryption/decryption switch signal indicates encryption,

performs decryption if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CBC mode, or

performs encryption if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CFB mode.

30. (Previously presented) An encryption/decryption device comprising:

a data structure analysis block for receiving encrypted data or data to be encrypted, analyzing the structure of the data and outputting information related to encryption as control data, the data structure analysis block also outputting the encrypted data or the data to be encrypted as processing block input data;

a data control block for outputting an encryption/decryption switch signal indicating which one of encryption and decryption should be performed, and a mode selection signal indicating in which mode the processing block input data should be processed, according to the control data;

a shared processing block configured to have the ability to perform encryption and decryption in either of the CBC mode and the CFB mode by performing ECB processing using input key data, the shared processing block performing encryption or decryption according to the encryption/decryption switch signal for the processing block input data in the mode indicated by the mode selection signal, and outputting encrypted result or decrypted result;

a first input selector for selecting encrypted data or the output of the shared processing block and outputting the selected data to the data structure analysis block;

a second input selector for selecting data to be encrypted or the output of the shared processing block and outputting the selected data to the data structure analysis block; and

an output selector for selecting a predetermined value or the output of the shared processing block and outputting the selected data,

wherein once processing in the shared processing block is performed for the encrypted data or the data to be encrypted for a predetermined number of times, the output selector selects the output of the shared processing block.

31. (Previously presented) The encryption/decryption device of Claim 30, wherein the predetermined number of times is three times.

32. (Previously presented) An encryption device comprising:

a data structure analysis block for receiving data to be encrypted, analyzing the structure of the data to determine control data and outputting the control data, the data structure analysis block also outputting the data to be encrypted as processing block input data;

a data control block for outputting a mode selection signal indicating in which mode the processing block input data should be processed, according to the control data; and

a shared processing block configured to have the ability to perform encryption in either of the CBC mode and the CFB mode by performing ECB processing using input key data, the shared processing block performing encryption for the processing block input data in the mode indicated by the mode selection signal and outputting encrypted result,

wherein the shared processing block comprises:

an ECB processor for performing the ECB processing and outputting the result as cipher-processed data;

a first selector for selecting one of the processing block input data and the cipher-processed data according to the mode selection signal, and outputting the selected data;

a delay device for delaying the cipher-processed data received as an input and outputting the delayed data;

a second selector for selecting one of the processing block input data, initial vector data and the delayed cipher-processed data output from the delay device according to the mode selection signal, and outputting the selected data;

an XOR operator for computing XOR of the output of the first selector and the output of the second selector and outputting the computed result;

a third selector for selecting one of the processing block input data, the output of the XOR operator and the delayed cipher-processed data according to the mode selection signal, and outputting the selected data;

a bit mask device for masking part of the key data as required according to the mode selection signal and outputting the result as mode-adaptive key data; and

a fourth selector for selecting one of the cipher-processed data and the output of the XOR operator according to the mode selection signal, and outputting the selected data as the encrypted result, and

the ECB processor performs encryption as the ECB processing for the output of the third selector using the mode-adaptive key data, and outputs the result as the cipher-processed data.

33. (Previously presented) A decryption device comprising:

a data structure analysis block for receiving encrypted data, analyzing the structure of the data and outputting information related to encryption as control data, the data structure analysis block also outputting the encrypted data as processing block input data;

a data control block for outputting a mode selection signal indicating in which mode the processing block input data should be processed, according to the control data; and

a shared processing block configured to have the ability to perform decryption in either of the CBC mode and the CFB mode by performing ECB processing using input key data, the shared processing block performing decryption for the processing block input data in the mode indicated by the mode selection signal and outputting decrypted result,

wherein the shared processing block comprises:

an ECB processor for performing the ECB processing and outputting the result as cipher-processed data;

a delay device for delaying the processing block input data received as an input and outputting the delayed data;

a second selector for selecting one of the processing block input data, initial vector data and the delayed processing block input data output from the delay device according to the mode selection signal, and outputting the selected data;

an XOR operator for computing XOR of the cipher-processed data and the output of the second selector and outputting the computed result;

a third selector for selecting one of the processing block input data and the delayed processing block input data according to the mode selection signal, and outputting the selected data; and

a bit mask device for masking part of the key data as required according to the mode selection signal and outputting the result as mode-adaptive key data, and

the ECB processor performs either encryption or decryption as the ECB processing for the output of the third selector using the mode-adaptive key data according to the mode selection signal, and outputs the result as the cipher-processed data.

34-37. (Canceled)